2015

Mapping the laws which apply to intercepting wireless communications in a Western Australian legal context

Tim Thomas

Craig Valli
Security Research Institute, Edith Cowan University, c.valli@ecu.edu.au

DOI: 10.4225/75/57b3f2f0fb886
13th Australian Digital Forensics Conference, held from the 30 November – 2 December, 2015 (pp. 22-36), Edith Cowan University Joondalup Campus, Perth, Western Australia.

MAPPING THE LAWS WHICH APPLY TO INTERCEPTING WIRELESS COMMUNICATIONS IN A WESTERN AUSTRALIAN LEGAL CONTEXT

Tim Thomas, Craig Valli
Edith Cowan University, Security Research Institute, Perth, Australia
sri@ecu.edu.au

Abstract

The rapid evolution and deployment of WiFi technology creates a new environment where offenders can intercept and obtain sensitive information for use in the commissioning of further criminal activity. This paper explores how the law applies to and protects the wireless communications environment, with specific focus on the interception of WiFi data communications.

Keywords
WiFi, data interception, data compromise, wireless security, wireless and the law.

INTRODUCTION

Wireless communication infrastructure is now commonplace in Western Australia. Advances in technology, cheaper production of wireless hardware coupled with the convenience of wireless and the demand for Internet based data services has driven a wireless infrastructure which focuses on ease of use and breadth of accessibility. In short the community wants cheap, no fuss data delivered seamlessly to all their devices, the technology and supporting industry are now able to deliver this. The scale of this paradigm shift is substantial. In the last decade we have moved from analogue modem connected desktop computers and restrictive access models to a multi-device, information based infrastructure which delivers cost effective services which are purchased at a granular level. The Australian Bureau of Statistics reports that Proportion of subscribers by connection type using wireless to access the Internet was the lowest at 1.7% in 2006. However, by Jun 2014 this was now the highest category of access at 48.1% of all users (Anonymous, 2014).

Whilst there are advantages to this system, not the least being a shift to consumer driven services, the desire for seamless operation, ease of use and wide deployment has created an environment where the ability to undertake actions could breach legal or ethical boundaries. Just because we can do something does not mean we should, and in many cases users may be unaware of the question, let alone the answer.

This paper will explore how the law in Western Australia applies to the most commonly deployed forms of consumer wireless infrastructure with a brief consideration of ethical issues. The paper will primarily focus on the issues relating to the interception of wireless data traffic.

What are the boundaries of this paper?

Wireless technology is a deceptively broad topic, encompassing everything from first generation mobile phones to the proprietary commercial architectures which underpin national critical infrastructure systems, which includes satellite and microwave systems.

The objective of this paper is to explore the wireless environment which is directly used by the general community and can be intercepted by the general community using common off the shelf (COTS) wireless equipment.

This paper will not explore systems which require specialist skills, equipment or access to intercept. Nor will this paper include the telephony system, which is a topic unto itself, with the exception of Voice Over IP telephony (VoIP) which is simply consumer grade voice data travelling over the Internet.

The wireless environment

Technology is now an affordable consumable item for general society. Australians in particular are particularly enthusiastic consumers, with 12,483,000 Internet subscribers at the end of June 2014 (Anonymous, 2014). In response to this demographic the technology industry has made their products easy to consume and use. As technology and service delivery has advanced, the underlying complexity of the systems has increased.

Consider for example a normal user who owns an Apple iPad, an Android phone, and a desktop computer, with WiFi enabled ADSL routers at their home and workplace. This user is allowed to work from home and use their own equipment at their office, which has implemented a Bring Your Own Device (BYOD) system. From the users perspective they have a single set of contacts, work and personal email accounts, and some documents they are working on. Each of these is available to them on any of their devices interchangeably. It is a perfectly natural and logical environment that a user would conduct business or leisure in today.

This user is unaware that their devices are repeatedly swapping between connection methods and network access points as they move around. Connection methods will change as signal strength fluctuates, with preference given to WiFi connections over 3G or 4G networks provided by the end users telephony providers. On top of this their data is being synchronised and stored to one or more locations on the Internet, the geographical locations of which are often unknown and could shift as the supplier balances load and storage.

In short, the wireless environment can be abstracted into two distinct layers from an end users perspective, a highly complex and sophisticated technical layer, concealed beneath an easy to use, fully featured user layer.

Intercepting wireless data

Wireless interception technology has developed commensurately with the rest of the wireless environment. That is, wireless interception tools are readily available and easy to use, freely downloadable from the Internet. Also how to perform wireless intercepts using these tools is also readily available from streaming services such as YouTube. Arguably, this abundance of tools and training creates the impression that it is acceptable to intercept wireless data. A user who is considering intercepting wireless data is not confronted with obstacles. From the comfort and security of their own home they can download a suite of tools, and conduct and interception with very little effort or technical knowledge simply following lock step one of the instructional videos online

Wireless in the form of WiFi 2.4Ghz is common and 5Ghz is gaining in popularity. Users are surrounded by large numbers of wireless networks, many of which are unsecured and even advertised as free services. Many commercial enterprises will offer free wireless access for customers across a range of industries. Whole of area coverage are now commonly promoted as desirable services which raise a group or body above their peers.

Users of wireless are required to explore their wireless environment. They must choose WiFi networks to connect to and may have to choose which wireless channel to use. These obligatory activities cast the user into a technician role.

A person who wants to intercept wireless is not confronted with the obstacles inherently associated with criminal or undesirable behaviour. They do not have to creep around in the dark, lie, or confront barriers to action such as the licensing obligations associated with acquiring a firearm. The evils of wireless interception do not feature strongly as plot lines in popular media or the news. To the general community the wireless environment is benign, and by association wireless interception may be perceived the same way.

Why would a person want to intercept wireless ?

A person could be motivated to intercept wireless for a number of reasons. It could be simple curiosity, or the desire to use more tools and feel more technical. A user could be troubleshooting a problem with their network or using it as an interdiction to see exactly what data is leaving and entering a network.

Investigative occupations such as law enforcement are information driven, and wireless traffic is information. Intercepting and interpreting wireless data could give investigators information about what a person is thinking, what they are doing, when they are doing it and who they are doing it with.

In addition there are criminal motives. These range from the desire to use a wireless service without paying, which could require an interception to discover the access information, to exploring and perhaps even taking information from another person's devices. The uses for stolen information are substantial and include identity theft, domestic spying, theft of financial information and gaining access information to corporate networks and remote storages.

The legal environment

Technology is developing faster than the law. The law represents the will and standards of the people, it reflects the rules of society. In most cases the law parallels societal ethics and morals. We think it is wrong to kill a person or steal their property so there are laws which punish people who do these things. By comparison

technology is a method, a facilitator or vehicle. Technology is how we do something, not what we do. In times past we used savings books to conduct our banking at the front counter of a bank, now we widely use the Internet to transact with the banking industry. Technology has not created a new set of actions, just provided a new, more convenient and cheaper way to do the same thing.

The law and technology do not evolve synchronously, in many cases the law responds as technology creates new ethical and moral issues which trouble society. Consequently finding the laws which relate to technological situations, and subsequently applying those laws will often require the user to think in two paradigms. Furthermore, laws which relate to wireless interception are detailed in both Western Australia and Commonwealth legislation.

When are you allowed to intercept wireless data?

Ultimately, a person can legally intercept wireless data if they have a codified lawful authority to do so or if there are no laws which make it illegal for them to do so.

The laws which relate to wireless interception are explored later in this paper.

Societal values

Australian society values safety and privacy, and these values should be taken into account when considering this topic. A person who enters another's house without permission or some other form of reasonable justification, such as to save a life, is wrong in the eyes of our society and our laws. A person's home is their castle, a fundamental tenant of most legal systems. Consider this in terms of a wireless network. Most wireless networks are created as part of the home environment. They are by logical extension just another part of the castle. To the people who live in that house the system is no different to any fixings or furniture within the house. In some respects the system may even be perceived as more private because the information it contains is not directly visible, like the pictures on the walls or the mail on the kitchen bench.

The technological knowledge, aptitude, and interest of the owners will determine the technological security of the wireless network. Unfortunately the desire to deliver hassle free easy to use systems comes at a price, the technical understanding of which would elude most users (Szewczyk, 2006). Whilst greater range and power means access is available throughout the house and garden, it also means the wireless network reaches across the road, into the neighbours, and maybe into the park. Manufacturers make their networks easy to find and join, a benefit which extends to anyone who can see the network, not just the owners.

The visibility and security of a wireless network do not necessarily reflect owner's choice about the security. Rather, they are a reflection of the technology which has been used and the skill and knowledge of the user. A person with an unsecured wireless network could be a private person. They may have no idea that their wireless network is broadcasting to the rest of their neighbourhood. As far as they are concerned they can stream video to an iPad in their back garden. Lack of technical awareness does not mean a person has decided to make their network freely accessible, much the same as leaving a door unlocked does not mean that a person has decided to allow free access to their house. Few people implement a personal wireless network with the intention of making it, and all the data it contains, available to the general public.

Should our values guide our choices in this situation or is the absence of a legal punishment sufficient to justify an action which breaches the ethics of our society? Whilst this paper is not a philosophical study, it will occasionally raise value based considerations, to inform the debate.

THE TECHNOLOGICAL STRUCTURE

For the purposes of this paper it is useful to separate wireless infrastructure into two groups, consumer wireless networks and commercial wireless networks. These groups generally correspond with the division between Western Australia law and Australian Commonwealth law. The schematic *"Wireless Connections To The Internet"* at figure 1 presents these two groups in the context of connections to the Internet.

Group 1 – Consumer wireless networks

This group consists of the WiFi networks, being systems specified under standards 802.11a to 802.11ac inclusive. The radio equipment in this group use 2.4 GHz and 5 GHz radio waves. This group is the range of frequencies used for the transmission of data, particularly Internet traffic.

This radio equipment is commonly installed in ADSL wireless routers, wireless access points, wireless extenders, mobile telephones, tablets, computers, wireless adaptors, network attached storage devices and other ancillary devices such as printers, gaming consoles and even white goods.

These devices can form part or all of a local area network, and can even be a node or component of a larger network, the reach of which can be International.

Group 2 – Commercial wireless networks

This group consists of the commercial networks which underpin the majority of the world's networks. These networks consist of a wide range of wired and wireless components which interoperate to supply seamless data transfers between networks. These are licensed spectrum and typically come under the management and enforcement of the Australian Communication and Media Authority (ACMA), who are responsible for managing commercial wireless spectrum.

The wireless components of these networks include 1G, 2G, 3G, 4G, microwave and satellite infrastructure.

The technological structure expressed in terms of connections.

For the purposes of this paper it is most useful to consider the infrastructure in terms of the way wireless data connections are made. The most common forms of connection, as displayed in figure 1, are described below:

Connection via an ADSL wireless router

A WiFi enabled device connects to an ADSL wireless router. The ADSL router connects to the Internet Service Provider (ISP) with whom the user holds an account over the wired telephone system or PTSN. This type of infrastructure is commonly found in homes and businesses, including businesses supplying free WiFi to their customers.

Direct 3GG/4G connection

A device with 3G/4G capability connects to the 3G/4G network and the carrier with whom they have an account directs their traffic to the Internet. Devices with 3G/4G connection capability include smart phones, tablets and computers with a 3G/4G adaptor and some providers provide static gateway devices

This type of infrastructure is very common. Most smart phones and a large proportion of tablets have the capability, with limitations being related to the type of account held by the user with their carriage service provider rather than the equipment.

Connection via a wireless hotspot

A WiFi enabled device connects to a WiFi hotspot. The WiFi hotspot connects to the ISP with whom the user holds a connection account over a 3G/4G connection. The main difference between a wireless hotspot and an ADSL router is the type of connection the device makes to the carriage service provider. ADSL routers use the wired telephone system whilst WiFi hot spots use the 3G/4G mobile network.

This type of infrastructure is becoming more common as 4G speed, pricing and mobility combine into an appealing proposition for consumers.

Connection via a 3G/4G enabled mobile device

A WiFi enabled device connects to a data enabled mobile device. The data enabled mobile device connects to the ISP with whom the user holds a connection account over a 3G/4G connection. This connection type is essentially the same as a wireless hotspot. Most new smartphones and tablets include the ability to tether, or "share" their Internet connection with other devices.

This type of infrastructure is common, and its use will grow as consumers exploit the speed of 4G, the economic advantage of a single data connection account, and the device mobility.

The technological structure – where will an interception occur? Where is the WiFi?

This paper focuses on the interception of data which is being transmitted over WiFi networks. Where then are the WiFi networks?

As displayed in figure 1, the only connections which do not involve WiFi are those which are made directly from 3G/4G enable device, such as a mobile telephone or tablet.

All other connections have a WiFi component, including tethering, which occurs when a 3G/4G enabled device shares its Internet connection with WiFi devices. In this scenario WiFi is used to make the connection between the 3G/4G device and the other device. The 3G/4G device can do this because it contains 3G/4G radio transceivers and WiFi radio transceivers.

Any WiFi connection can be intercepted using commonly available equipment, such as a device with a WiFi radio transceiver and software which can be downloaded for free.

A word on encryption

Wireless technology implements encryption to protect the data it is transmitting and compression to improve the speed and efficiency of its operation. It is one thing to intercept a wireless data transmission; it is another thing to read it.

Whilst this paper does not deal with this issue, it is prudent to note that the current state of technology makes breaking WiFi encryption a simple process. All forms of security utilised by consumer grade devices WEP, WPA, WPA2 can be readily broken (Tsitroulis, 2014) (Valli & Wolski, 2004) These breaks are well documented in the cyber security literature. Furthermore video sharing sites such as youtube have tutorials on how to break these encryption schemes using existing common off the shelf (COTS) hardware and freely downloadable software.

The legal component of this paper will identify if reading a data transmission is necessary for an offence to occur.

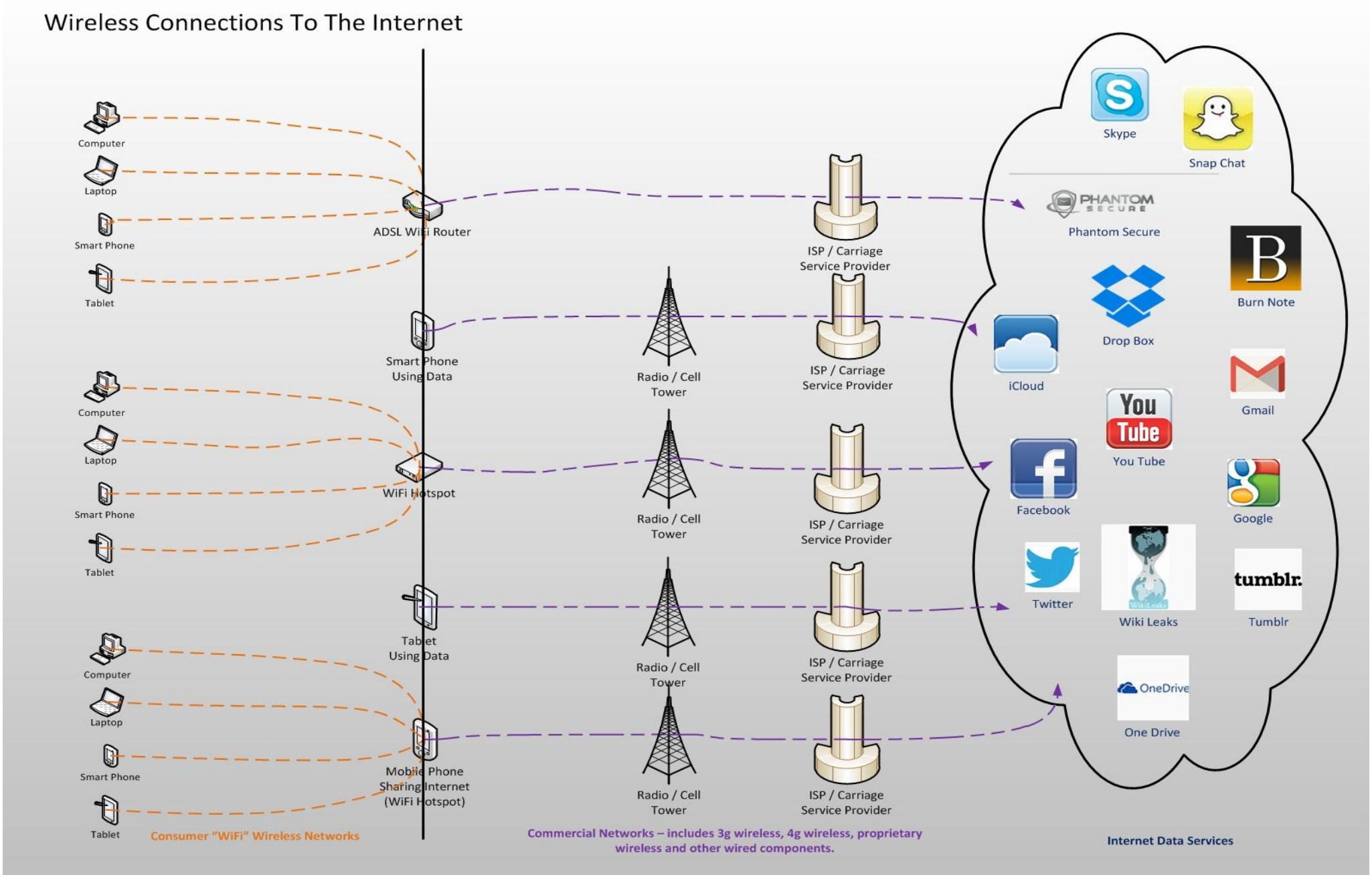
Wireless Connections To The Internet
Computer
Laptop
Smart Phone
Tablet
ADSL Wi-Fi Router
Smart Phone Using Data
Computer
Laptop
Smart Phone
Tablet
WiFi Hotspot
Tablet Using Data
Computer
Laptop
Smart Phone
Tablet
Mobile Phone Sharing Internet (WiFi Hotspot)
Consumer "WiFi" Wireless Networks
Radio / Cell Tower
Radio / Cell Tower
Radio / Cell Tower
Radio / Cell Tower
ISP / Carriage Service Provider
ISP / Carriage Service Provider
ISP / Carriage Service Provider
ISP / Carriage Service Provider
Commercial Networks – includes 3g wireless, 4g wireless, proprietary wireless and other wired components.
Skype
Snap Chat
Phantom Secure
Burn Note
Drop Box
iCloud
Gmail
You Tube
Facebook
Google
Twitter
Wiki Leaks
Tumblr
One Drive
Internet Data Services

Figure 1

THE LEGAL STRUCTURE

Which laws?

As previously stated a person can legally intercept wireless data transmissions if they have a codified lawful authority to do so or if there are no laws which make it illegal for them to do so. This paper will focus on the laws which:

- Make it unlawful to intercept data being transmitted over wireless
- Provide a lawful authority to intercept data being transmitted over wireless

This paper will address the laws as they apply to the general community. Law enforcement powers are a complex area which exceeds the scope and purpose of this paper. It is sufficient to note that law enforcement are bound by the same laws and restrictions as the general community, and rely on special exemptions and powers which are frequently controlled by the application of a judicial test.

Covering the field

Two sets of law can apply in Western Australia, laws made by the state of Western Australia and laws made by the Commonwealth Of Australia. When laws from each of these jurisdictions relate to the same topic the Constitution Of Australian specifies which law is applied. This is referred to as the "covering the field test", and is set out in Section 109 of the Constitution Of Australia which states:

> When a law of a state is inconsistent with a law of the Commonwealth, the latter shall prevail, and the former shall, to the extent of the inconsistency, be invalid.

This paper will take covering the field into account.

Commonwealth Laws

The Commonwealth Law covers the field in relation to telecommunications infrastructure, which have been described in this paper as "Commercial Networks". The Telecommunications Act 1997 (Cth) and the Telecommunications Interceptions and Access Act 1997 (Cth) in particular clearly and comprehensively cover this area.

However, the Commonwealth Law is also complex, difficult to piece together and undergoing change in response to the rapidly changing landscape. The largest questions relate to exactly how far they go.

The Commonwealth Telecommunications Acts'

The following definitions from Section 7 (definitions) of the Telecommunications Act 1997 (Cth) are instructive.

> Telecommunications network means a system, or series of systems, that carries, or is capable of carrying, communications by means of guided and/or unguided electromagnetic energy.
>
> Communications includes any communication:
>
> (a) whether between persons and persons, things and things or persons and things; and
> (b) whether in the form of speech, music or other sounds; and
> (c) whether in the form of data; and
> (d) whether in the form of text; and
> (e) whether in the form of visual images (animated or otherwise); and
> (f) whether in the form of signals; and
> (g) whether in any other form; and
> (h) whether in any combination of forms.

Wireless data communications of all types meet this definition and gives insight into the intentions of the legislators. The key question which needs to be answered is does the Commonwealth legislation make it unlawful to intercept wireless data communication. Section 7 of the Telecommunications (Interceptions and Access) Act 1979 (Cth) states:

7 Telecommunications not to be intercepted

(1) A person shall not:
  (a) intercept;
  (b) authorize, suffer or permit another person to intercept; or
  (c) do any act or thing that will enable him or her or another person to intercept;
a communication passing over a telecommunications system.

Interpreting this section requires clarification of the following terms, which are found in Section 5 (definitions) of the Telecommunications (Interceptions and Access) Act 1979 (Cth):

> Communication includes conversation and a message, and any part of a conversation or message, whether:
> (a) in the form of:
> (i) speech, music or other sounds;
> (ii) data;
> (iii) text;
> (iv) visual images, whether or not animated; or
> (v) signals; or
> (b) in any other form or in any combination of forms.
>
> Telecommunications system means:
> (a) a telecommunications network that is within Australia; or
> (b) a telecommunications network that is partly within Australia, but only to the extent that the network is within Australia;
> and includes equipment, a line or other facility that is connected to such a network and is within Australia.
>
> Telecommunications network means a system, or series of systems, for carrying communications by means of guided or unguided electromagnetic energy or both, but does not include a system, or series of systems, for carrying communications solely by means of radiocommunication.
>
> Telecommunications service means a service for carrying communications by means of guided or unguided electromagnetic energy or both, being a service the use of which enables communications to be carried over a telecommunications system operated by a carrier but not being a service for carrying communications solely by means of radiocommunication.

And these definitions in the Telecommunications (Interception) Amendment Act 2006 (Cth):

5F When a communication is passing over a telecommunications system

> For the purposes of this Act, a communication:
> (a) is taken to start passing over a telecommunications system when it is sent or transmitted by the person sending the communication; and
> (b) is taken to continue to pass over the system until it becomes accessible to the intended recipient of the communication.

5H When a communication is accessible to the intended recipient

(1) For the purposes of this Act, a communication is accessible to its intended recipient if it:
  (a) has been received by the telecommunications service provided to the intended recipient; or
  (b) is under the control of the intended recipient; or
  (c) has been delivered to the telecommunications service provided to the intended recipient.

These sections make it clear that the interception of a telecommunication is unlawful. Whilst Section 7, which creates the offence, goes on to list exemptions to the law, these principally relate to service technicians and installers in certain circumstances and have not been included in this paper in the interests of brevity. Suffice it to say that general members of the public are not on the list.

Law enforcement seeking an exemption from this law must satisfy a significant judicial burden to obtain the power to intercept telecommunications. Furthermore, all information obtained from an interception is subject to rigorous storage, access and auditing requirements. This demonstrates the legislators' view, that interception of telecommunications is a serious and restricted power.

Two other issues should be considered:

- The definition of a telecommunications network excludes radio communications, and
- When does a telecommunication pass outside the scope of the legislation?

The definition of a telecommunications network excludes radio communications

Section 5 of the Telecommunications (Interceptions and Access) Act 1979 (Cth) states:

> Telecommunications network means a system, or series of systems, for carrying communications by means of guided or unguided electromagnetic energy or both, but does not include a system, or series of systems, for carrying communications solely by means of radio communication.

In this definition the term radio communications is limited in its application to *systems for carrying communications solely by means of radio communication*. Whilst the limitation clearly applies to television, radio and radar, the author i unable to find any telecommunication system, particularly those which carry data, which are exclusively comprised of radio communication equipment.

It is likely this wording was included to enforce the delineation between the telecommunications legislation and the Radio communications Act 1992 (Cth), which focuses on the management of the radio spectrum and does not appear to contain any offences for intercepting communications. This is reasonable since it is intended that radio and television communications are intercepted.

Consequently it is reasonable to propose that the legislators intended that data communications be covered by the telecommunications laws, and that the composition of the telecommunications infrastructure is a significant inclusive factor.

When does a communication pass outside the control of the legislation?

A telecommunication moves outside the control of the telecommunications legislation when it becomes accessible to the intended recipient, which occurs when one of the conditions stated in Section 5H of the Telecommunications (Interceptions and Access) Act 1979 (Cth) occurs. Section 5H states:

5H When a communication is accessible to the intended recipient

> (1) For the purposes of this Act, a communication is accessible to its intended recipient if it:
>
> (a) has been received by the telecommunications service provided to the intended recipient; or
>
> (b) is under the control of the intended recipient; or
>
> (c) has been delivered to the telecommunications service provided to the intended recipient.

Subsection (1)(b) is the most direct part of this law, stating that a communication is accessible to its intended recipient once it is under the control of the intended recipient. When assessing these criteria it is important to determine when the communication is no longer under control of the telecommunications service provider. It is reasonable to propose that this occurs once the communication reaches the recipients WiFi network. At this point the communication passes onto equipment owned and configured by the intended recipient, which is outside the control of the network service provider. This proposition is supported by the nature of the infrastructure, where the transition point could be the final technical destination, as is the case when the communication is received by a 3G smart phone, or a routing point controlled by the user, as is the case with a 3G smart phone which is operating as a wireless router servicing a desktop computer. In either scenario the service provider has no knowledge or control over what is occurring beyond the 3G smartphone.

Other Commonwealth Acts

Divisions 476, 477 and 478 of the Criminal Code Act 1995 (Cth) provide a range of offences relating to computers and computer communications.

The offence of Obtaining Data set down in Section 478.4 could be applied to intercepting wireless data communications, but does require that the data be obtained with the intention of using the data to commit an

offence in Division 477, which includes offences for Unauthorised Access, Impairment and Modification. This would include intercepting data for the purpose of obtaining passwords which the interceptor intended to use to access the system.

Of particular note, Section 476.4 states that the laws in this Part of the Criminal Code Act 1995 (Cth) do not exclude or limit the operation of a State law. In other words, whilst these laws create a set of computer related offences which could be applied in Western Australia, they do not cover the field.

WESTERN AUSTRALIA LAWS

The Criminal Code Act Compilation Act 1913 (WA)

Section 440A of the Criminal Code Act Compilation Act 1913 (WA) creates an offence for unlawfully using a computer. Section 440A states:

440A. Unlawful use of computer

(1) In this section, computer system includes

(a) a part of a computer system;

(b) an application of a computer system;

Password includes a code, or set of codes, of electronic impulses;

Restricted-access computer system means a computer system in respect of which

(a) the use of a password is necessary in order to obtain access to information stored in the system or to operate the system in some other way; and

(b) the person who is entitled to control the use of the system

(i) has withheld knowledge of the password, or the means of producing it, from all other persons; or

(ii) has taken steps to restrict knowledge of the password, or the means of producing it, to a particular authorised person or class of authorised person;

Use a computer system means

(a) to gain access to information stored in the system; or

(b) to operate the system in some other way.

(2) For the purposes of this section a person unlawfully uses a restricted-access computer system

(a) if the person uses it when he or she is not properly authorised to do so; or

(b) if the person, being authorised to use it, uses it other than in accordance with his or her authorisation.

(3) A person who unlawfully uses a restricted-access computer system is guilty of a crime and is liable

(a) if by doing so the person

(i) gains a benefit, pecuniary or otherwise, for any person; or

(ii) causes a detriment, pecuniary or otherwise, to any person,

of a value of more than $5 000, to imprisonment for 10 years;

(b) if by doing so the person

(i) gains or intends to gain a benefit, pecuniary or otherwise, for any person; or

(ii) causes or intends to cause a detriment, pecuniary or otherwise, to any person,

to imprisonment for 5 years;

(c) in any other case, to imprisonment for 2 years.

To apply Section 440A to the interception of wireless data requires a broad interpretation of the definition of a computer system. Specifically, a computer system must be a system of computers, of which a wireless network is a part. The scope to apply this wide interpretation is assisted by the use of the word “includes” in the definition, which opens rather than closes the definition. Furthermore the intention of the legislators in this

instance is clearly to protect computer systems and the information they contain, which also supports the application of this law to unauthorised WiFi data interceptions.

Section 440A also requires that access to the computer system be restricted by the requirement to use codes. The implementation of WPA or WEP on a wireless router would meet this requirement.

The Criminal Code also includes a wide range of other offences, such as Fraud in Section 409, which can be applied to events closely related to data interceptions. These offences focus on the information, finances or intentions of the offender rather than the technical infrastructure.

JOINING THE TECHNOLOGICAL AND LEGAL

Which laws apply where?

In order to better understand the relationships between the technological infrastructure and the laws, the information identified in this paper have been set out in schematic and tabular format.

The schematic at Figure 2 graphically portrays which laws apply where on the technological infrastructure.

The table at Figure 3 sets out common scenarios, the laws which apply, and any issues which need to be considered.

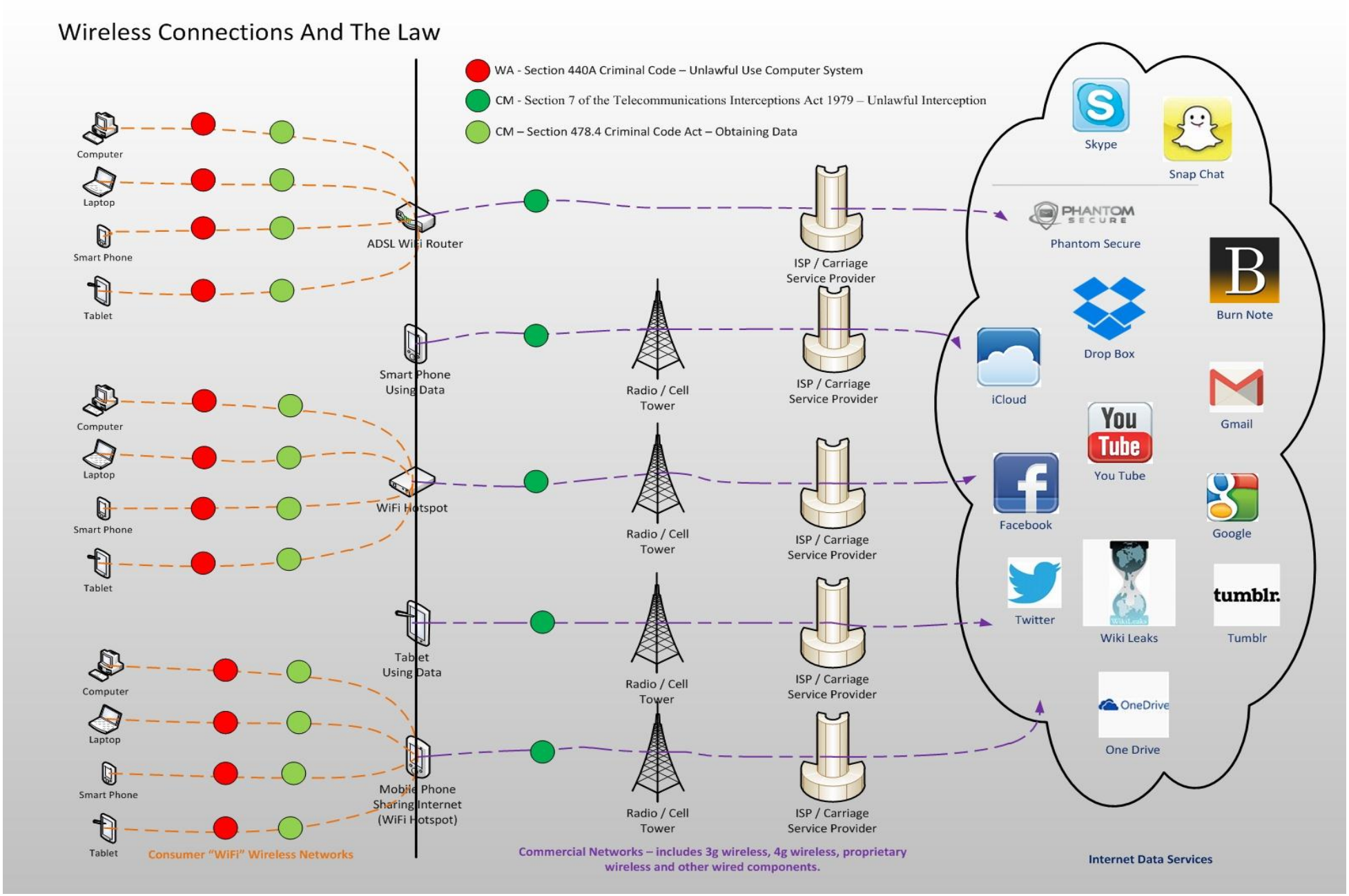
Wireless Connections And The Law
WA - Section 440A Criminal Code – Unlawful Use Computer System
CM - Section 7 of the Telecommunications Interceptions Act 1979 – Unlawful Interception
CM – Section 478.4 Criminal Code Act – Obtaining Data
Computer
Laptop
Smart Phone
Tablet
ADSL WiFi Router
Smart Phone Using Data
Computer
Laptop
Smart Phone
Tablet
WiFi Hotspot
Tablet Using Data
Computer
Laptop
Smart Phone
Tablet
Mobile Phone Sharing Internet (WiFi Hotspot)
Consumer "WiFi" Wireless Networks
Radio / Cell Tower
Radio / Cell Tower
Radio / Cell Tower
Radio / Cell Tower
ISP / Carriage Service Provider
ISP / Carriage Service Provider
ISP / Carriage Service Provider
ISP / Carriage Service Provider
Commercial Networks – includes 3g wireless, 4g wireless, proprietary wireless and other wired components.
Skype
Snap Chat
Phantom Secure
Burn Note
Drop Box
iCloud
Gmail
You Tube
Facebook
Google
Twitter
Wiki Leaks
Tumblr
One Drive
Internet Data Services

Figure 2

#	Scenario	Laws Broken	Points Of Note
1	A person uses a WiFi enabled device to intercept WiFi data from a WiFi network without the knowledge or authority of the owner. The owner of the WiFi network has implemented a password on the WiFi network and keeps knowledge of this password to themselves. The intercepting person collects a serious of packets and is able to read the contents. It doesn't matter if the person has to perform additional actions to interpret the data.	Section 440A of the WA Criminal Code Possibly Section 478.4 of the CM Criminal Code	An offence against the Commonwealth Code also occurs if the person intercepted the data for the purposes of committing some other offence.
2	As scenario one, but in this instance the person conducting the intercept does so for the purposes of obtaining passwords so they can access network directly.	Section 440A of the WA Criminal Code Section 478.4 of the CM Criminal Code	A more realistic scenario, as persons capturing WiFi data do so for a purpose.
3	A person uses a WiFi enabled device to intercept WiFi data from a WiFi network without the knowledge or authority of the owner. The owner of the WiFi network has not implemented a password on the WiFi network. The intercepting person collects a serious of packets and is able to read the contents. It doesn't matter if the person has to perform additional actions to interpret the data..	None identified	This scenario identifies an apparent deficit in the law. Whilst the legislators at both Commonwealth and State levels have enacted laws which protect the security of data communications, it appears the rapid evolution and deployment of WiFi infrastructure has outpaced the law. In this instance the victim's technical ignorance prevents the law from applying.
4	As scenario three, but in this instance the person conducting the intercept does so for the purposes of obtaining passwords so they can access network directly.	Section 478.4 of the CM Criminal Code	In this instance Section 440A does not apply as the WiFi network was not a restricted access system.
5	A person uses a WiFi enabled device to capture WiFi data on their own WiFi system. The persons could be curious, troubleshooting their network, testing their network or examining their security. In this situation it is immaterial if there is, or is not a password.	None identified.	An offence is not committed against Section 440A because their actions were authorised. An offence is not committed against Section 478.4 as there was no intention to commit another offence.
6	As scenario 5, but in this instance the person accidentally captures traffic from a neighbour's network which is protected by a password.	Section 440A of the WA Criminal Code	Whilst the person has a defence of accident to the offence, it is the judicial systems role to assess the validity of the claim. It is not uncommon for offenders to break the law then pretend it was an accident or mistake. It is likely that a court assessing a defence of this nature would expect a duty of care.

Figure 3

DISCUSSION AND CONCLUSION

The evolution of technology and the evolution of the law

Technology is evolving faster than the law. This statement is understandable as each of these areas has different drivers for change. Technology change is driven by business competition, community desires, efficiency, potential, and above all economics. Legal change is driven by several factors including politics, community expectations and outright necessity.

Technological evolution is fast because it can be and because there are profits to be made in being first to market. Legal evolution is slow because it should be, political debate should occur and impacts on existing frameworks established.

This paper has found one area where the law appears to have fallen behind technology, namely the absence of laws to protect the technologically ignorant who implement WiFi networks without a password or poor security.

This paper has also found that in the majority of circumstances there are laws which prevent the interception of data being transmitted over wireless.

The intentions of the legislators

When considering the law the intentions of the legislators should always be taken into account. It is quite clear that the laws are intended to extend the same protections afforded to a person's home as to their communications. Whilst the laws in this area are currently clumsy, particularly as they seek to preserve the structures of traditional radio communication mediums such as radio and television, they are evolving and will become more exacting as time progresses. The intentions of the legislators tell us the direction they are likely to go, and this direction reflects the will of the community.

The intentions of law enforcement

Will the unauthorised interception of WiFi data cause a law enforcement investigation? The answer to this lies in the intentions of law enforcement. The object of law enforcement is to keep the community safe, which includes protecting people's rights and property. Where a person did not want their data to be accessed then police would be likely to review the evidence to see if an investigation and subsequent prosecution was warranted.

This review would take into account a range of factors including accidental access, reckless behaviour on the part of the victim, the technical skill of all parties, and the automated behaviour of the technology. Ultimately if a person had done the wrong thing, for the wrong reasons, police would be likely to investigate due to intent. Starting an investigation does not mean however, that sufficient evidence will be found to support a charge. It simply means a matter will be investigated.

Other offences

Whilst this paper has identified a number of offences which can be applied to the interception of data from WiFi, it has not explored all the other offences which could be applied based on the other surrounding facts. It would be a mistake to assume that the laws identified in this paper are the only ones which can be applied. When law enforcement conducts an investigation they take all the facts into account. Investigation could reveal that technology was merely the facilitator for some other offence, such as fraud or stalking.

REFERENCES

ABS (2013) 8153.0 – Internet Activity, Australia, December 2013
http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/8153.0Chapter3December%202013

Achilleas Tsitroulis, Dimitris Lampoudis, Emmanuel Tsekleves. (2014) Exposing WPA2 security protocol vulnerabilities. *International Journal of Information and Computer Security*, 6 (1): 93

Anonymous. (2014). *8153.0 - Internet Activity, Australia, June 2014* Australian Bureau of Statistics Retrieved from http://www.abs.gov.au/ausstats/abs@.nsf/mf/8153.0/.

Commonwealth of Australia, (1979), Telecommunications (Interceptions and Access) Act 1979

Commonwealth of Australia, (1992). The Radiocommunications Act 1992

Commonwealth of Australia, (1995) The Criminal Code Act 1995

Commonwealth of Australia, (1997), The Telecommunications Act 1997

Commonwealth of Australia, (2006), The Telecommunications (Interception) Amendment Act 2006

State of Western Australia (1913), The Criminal Code Compilation Act 1913

Szewczyk, P. S. (2006). *Individuals' Perceptions of Wireless Security in the Home Environment.* Paper presented at the 4th Australian Information Security Management Conference, Perth, Western Australia.

Valli, C., & Wolski, P. (2004). *802.11b Wireless Networks Insecure at Any Speed*. Paper presented at the SAM'04, Las Vegas.